REMARKS

Status of the Claims

- Claims 1-2, and 4-13 are pending in the Application after entry of this amendment.
- Claims 1-2, and 4-13 are rejected by Examiner.
- Claims 1, 2, and 4-6 are amended by Applicant.

Claim Rejections Pursuant to 35 U.S.C. §103

Claims 1-2, 5, 7-8, 10, and 12-13 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Menezes "Handbook of applied cryptography" (Menezes) in view of U.S. Patent No. 6,763,112 to Haumont (Haumont).

Independent Claims 1 and 5 are amended to include the aspects that the data and an identifier for the data are received by a receiver and that the receiver does not know the identity of the transmitter. Support for this amendment is found on page 2 lines 14-19 and page 1, lines 9-20.

Menezes at p 402, lines 1-8, discloses an example of mutual authentication using random numbers. The example includes the following, in Menezes notation:

1. B → A: r_B
2. A → B: $E_K(r_A,r_B,B^*)$
3. B → A: $E_K(r_B,r_A)$

A: decrypts (3) and A checks that both random numbers in (2) match those used earlier.

Wherein:

- B→ A represent B transmitting to A
- E_K represents a symmetric encryption algorithm with a key K shared between A and B.

- r_A and r_B are random numbers for A and B respectively
- *B** is an identifier element.

As stated in Menezes p 401, para 10.16,where Menezes defines the terms used for the above:

"It is assumed that both parties are aware of the claimed identity of the other, either by context, or by additional (unsecured) clear text data fields." (See Menezes, 10.16).

However, pending Claim 1, using Menezes notation, can be expressed as:

1C. B→ A: data + r_B

2C. A→ B: r_A, r_B

3C. B→ A: $G(r_A, r_B)$

A: A applies a second function, H, to verify the result of $G(r_A, r_B)$ where G and H were given to B and A respectively by a third party.

Wherein:

- G represents a response computation function applied by B, where G is provided by a third party.
- H represents a computation function used by A, where H is provided by a third party.

It can thus be seen that Menezes fails to teach that B sends data (i.e. data + r_B) to A. Indeed, this is normal in the prior art, as data is usually not sent until after the devices have been authenticated. Thus, comparing steps 1 (from Menezes) and 1C (from Claim 1) above, it becomes evident that Menezes fails to disclose that A receives data and an identifier for the data in advance of authentication as is indicated by amended Claim 1.

In addition, whereas the present Claim 1 first sends the random numbers (step 2C) and then the result of a computation (function G) over the random numbers (step 3C), Menezes sends results of a computation (i.e. a symmetric key encryption) in both steps 2 and 3, albeit the order of the encryption is different in the two steps. Thus, there is an evident difference between the steps 1-3 in Menezes compared with claimed steps 1C-3C in Claim 1. Amended Claim 5 is likewise different from Menezes.

Furthermore, apart from the fact that Menezes does not explicitly teach transmitting data, nothing in Menezes indicates that the transmitter has been authorized to send data by the trusted third party. In Menezes, both parties A and B are aware of the identity of the other, and A even sends a "B identifier element", B*, to party B (see Menezes step 2, and section 10.16, page 401). This is in contrast to amended pending Claim 1 which explicitly indicates that the receiver does not know the identity of the transmitter. Also, in pending Claim 1, the first and second functions (identified as G and H in specification) are transmitted to the transmitter and receiver respectively from a trusted third party. This aspect is different from Menezes in which each of the parties knows each other's identity.

Thus, Menezes actually teaches away from the present invention because Menezes assumes receiver knowledge of the transmitter identity whereas pending amended Claim 1 states that the receiver does not know the identity of the transmitter.

Haumont describes a security procedure for use with a mobile communication service in a mobile communication system having a core network connected to a plurality of radio access networks respectively providing radio coverage over radio access network areas, each of the plural radio access networks having a radio network controller and a base station, said security procedure comprising the steps of:

- detecting, by a radio network controller a communication failure between the radio network controller and a mobile station, the radio network controller controlling radio coverage in a radio access network area in which the mobile station is located;

- transmitting a request from the radio network controller to the core network to perform an authentication of the mobile station; and
- performing a mobile station authentication procedure between the core network and the mobile station. (See Haumont, granted Claim 1).

Thus, Applicant understands that Haumont discusses that when a failure of a communication between a mobile station (A) and a radio network controller (B) occurs, then the radio network controller requests that an authentication be performed between the core network and the mobile station.

However, Haumont, like Menezes, also fails to discuss receiving the data and an identifier for the data from a transmitter as in the context of amended Claim 1.

When Menezes is modified by the addition of Haumont, then the combination produces a system where Menezes is modified such that if a communication failure between A and B were to occur then the receiver would request an authentication between another party, the core network, and the transmitter. Amended pending Claims 1 and 5 are functional without the extra authentication failure aspect of the combination of Menezes and Haumont.

Applicant respectfully submits that the combination of Menezes and Haumont cannot render obvious pending independent Claims 1 and 5 under 35 USC §103(a) as well as their respective dependent Claims 2 and 7-8, 10, and 12-13 per MPEP §2143.03 because Menezes teaches away from the claimed invention and all of the elements of the amended pending claims are not present in the combination of cited references.

Applicant respectfully requests reconsideration and withdrawal of the 35 USC §103(a) rejections on Claims 1-2, 5, 7-8, 10, and 12-13 in light of the arguments presented above.

Claims 4, 6, 9, and 11 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Menezes "Handbook of applied cryptography" (Menezes) in view of

U.S. Patent No. 6,763,112 to Haumont (Haumont), and in further view of U.S. Patent No. 5,815,665 to Teper et al. (Teper).

The teachings of Menezes and Haumont are discussed above.

Teper discusses an Online Brokering Service provides user authentication and billing services to allow users to anonymously and securely purchase online services from Service Providers (SP) sites (e.g., World Wide Web sites) over a distributed public network, which may be an untrusted public network such as the Internet. Users and SP sites initially register with the Brokering Service, and are provided with respective client and server software components for using the Brokering Service. In one embodiment, when a user initially connects to an SP site, the SP site transmits a challenge message over the public network to the user computer, and the user computer generates and returns and cryptographic response message (preferably generated using a password of the user). The SP site then passes the response message to the Brokering Service, which in-turn looks up the user's password and authenticates the response message. (See Teper, Abstract).

However, the addition of Teper to the combination Menezes and Haumont cannot overcome the aspect that Menezes teaches away from the claimed invention.

As a result, Applicant respectfully submits that the combination of Menezes, Haumont, and Teper cannot render obvious independent Claims 1 and 5 and their respective dependent Claims 4, 6, 9, and 11 under 35 USC §103(a) per MPEP §2143.03 because the combination of Menezes, Haumont, and Teper teach away from the present invention.

Conclusion

Applicant respectfully submits that the pending claims patentably define over the cited art and respectfully requests reconsideration and withdrawal of all rejections of the pending claims. Reconsideration for a Notice of Allowance for all pending claims is respectfully requested.

If there are any additional charges in connection with this requested amendment, the Examiner is authorized to charge Deposit Account No. 07-0832 therefore.

Respectfully submitted,
Eric Diehl
Jean-Pierre Andreaux
Alain Durand

Date: May 4, 2009

/Jerome G. Schaefer/

Jerome G. Schaefer
Attorney for Applicant
Registration No. 50,800
(609) 734-6451

Thomson Licensing, LLC
Patent Operation
PO Box 5312
Princeton, NJ 08543-5312